AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Cancelled)

2. (Previously Presented) A method according to claim 20, further comprising:
sending information specific to the second unit to the first unit before computing the application key in the first unit.

3. (Previously Presented) A method according to claim 20, further comprising:
sending a random number provided by the second unit to the first unit, before encrypting the application key in the first unit.

4. (Previously Presented) A method according to claim 20, further comprising:
sending information pertaining to an application key to the first unit, before encrypting the application key within said first unit.

5. (Previously Presented) A method according to claim 4, further comprising:
choosing the application key to be encrypted based on said information pertaining to an application key.

6. (Previously Presented) A method according to claim 20, wherein said encryption of an application key intended for a second unit is unique.

7. (Previously Presented) A method according to claim 20, further comprising:
verifying integrity of the data, wherein verifying the integrity of the data comprises verifying the encrypted application key.

8. (Previously Presented) A method according to claim 20, further comprising:
sending information pertaining to an application key to the second unit, before decrypting the encrypted application key within said second unit of said set.

9. (Previously Presented) A method according to claim 20, further comprising:
storing within the second unit, after decrypting the encrypted application key, said key within said second unit.

10. (Previously Presented) A method according to claim 9, wherein storing of the application key within the second unit is done based on information pertaining to an application key.

11. (Previously Presented) A method according to claim 20, further comprising:
verifying that the application key is authentic.

12. (Previously Presented) A method according to claim 20, wherein the first security unit comprises a smart card.

13. (Previously Presented) A method according to claim 20, wherein the memory comprises a rewritable memory.

14. (Previously Presented) A method according to claim 20, wherein a second unit comprises several application keys.

15. (Previously Presented) A method according to claim 20, wherein the first unit comprises several application keys.

16. (Previously Presented)A method according to claim 20, further comprising:
after encrypting the application key, erasing the operation key temporarily saved within a second volatile memory of the first unit.

17. (Previously Presented) A method according to claim 20, further comprising:
after decrypting the application key, erasing the operation key temporarily saved within a second volatile memory in the first unit.

18. (Previously Presented) A method according to claim 2, further comprising:
sending random information, information pertaining to an application key and the information specific to the second unit to the first unit by means of a first single command.

19. (Previously Presented) A method according to claim 20, further comprising:

sending the encrypted application key and information pertaining to an application key to the second unit by means of a second single command.

20. (Currently Amended) A method for customizing a set of several second security units, comprising:

secure downloading of an application key from a first security unit of a central processing unit to said set of second security units, said first unit and second units each comprising at least one memory, wherein the method further comprises for each second unit in said set:

on each downloading, computing an operation key in the first unit based on information specific to the second unit, a transport key, and a diversification algorithm, said transport key residing within the memory of the first security unit, said memory being non volatile;

encrypting the application key in the first unit based on information comprising said operation key and an encryption algorithm;

sending data comprising the encrypted application key to the second unit;

on each downloading, computing an operation key in the second unit based on information specific to the second unit, the transport key and the diversification algorithm, the same transport key residing in the non-volatile memory of each second security unit of said set, said operation key not being stored within the memory of said second unit; and

decrypting the encrypted application key in the second unit based on information comprising said operation key and a decryption algorithm which is the inverse of the encryption algorithm,

wherein said transport key residing within the memory of the first unit is present in the memory of the first unit prior to communicating with the second unit and the same transport key residing in the non-volatile memory of each second unit is present in the non-volatile memory of the second security unit prior to communicating with the first unit.

21. (Previously Presented) A method according to claim 3, further comprising:

sending random information, information pertaining to an application key and information specific to the second unit to the first unit by means of a first single command.

22. (Previously Presented) A method according to claim 4, further comprising:

sending random information, information pertaining to an application key and information specific to the second unit to the first unit by means of a first single command.

23. (Previously Presented) A method according to claim 2, further comprising:

sending the encrypted application key and information pertaining to an application key to the second unit by means of a single second command.